2 กันยายน 2569

เรียน ผู้จัดการ

สถาบันผู้ใช้บริการระบบบาทเนต

ที่ ธปท. 5324/2569 เรื่อง การนำส่งคู่มือ ธปท. และแนวปฏิบัติที่เกี่ยวข้อง พร้อมทั้งแผนการ Go-live Phase 1 ของโครงการ BAHTNET API

ตามที่ ธนาคารแห่งประเทศไทย (ธปท.) และสมาชิกผู้ใช้บริการบาทเนตได้ร่วมกันพัฒนา BAHTNET Application Programming Interface (BAHTNET API) เป็นช่องทางการทำธุรกรรมบาทเนต เพื่อลดการพึ่งพาเครือข่ายต่างประเทศ (Geopolitical Risk) และสนับสนุนการดำเนินธุรกรรมแบบ Straight Through Processing (STP) ตามทิศทางการพัฒนาระบบบาทเนต (BAHTNET NextGen) ที่ได้รับความเห็นชอบจากคณะกรรมการระบบการชำระเงิน (กรช.) และมีกำหนดการเริ่มใช้งานจริงในเดือนตุลาคม 2569 นั้น

ที่ผ่านมา ธปท. ได้วางแผนพัฒนาระบบ ปรับปรุงกระบวนการที่เกี่ยวข้อง และทดสอบร่วมกันกับสมาชิกผู้ใช้บริการบาทเนตที่เข้าร่วมโครงการมาอย่างต่อเนื่อง ซึ่งปัจจุบันมีความคืบหน้าเป็นไปตามแผนงานที่กำหนด โดยสมาชิกผู้ใช้บริการบาทเนตทุกสถาบันที่เข้าร่วมโครงการได้ผ่านการทดสอบ Functional Test และ Non-Functional Test เป็นที่เรียบร้อยแล้ว ทั้งนี้ เพื่อให้สมาชิกได้มีเวลาในการเตรียมการ ทั้งด้านเอกสาร และระบบงาน รวมทั้งลดความเสี่ยงจากปัญหาที่พบในการทดสอบความพร้อมช่วงเดือนตุลาคม 2569 ธปท. จึงได้แบ่งกำหนดการ Go-live ออกเป็น 2 Phases ดังนี้

- Go-live Phase 1 (เฉพาะ Function การเชื่อมต่อ): ในวันที่ 14 กันยายน – 9 ตุลาคม 2569 เพื่อให้สมาชิกเตรียมการด้านเอกสาร ระบบงาน และทำการเชื่อมต่อกับระบบ BAHTNET API ของ ธปท. บนระบบที่จะใช้งานจริง (Production)
- Go-live Phase 2 (ทุก Function ที่ให้บริการ): ในเดือนตุลาคม 2569 เพื่อเริ่มใช้งานในการทำธุรกรรมบาทเนตผ่านช่องทาง BAHTNET API

ดังนั้น เพื่อให้การ Go-live Phase 1 เป็นไปโดยราบรื่นตามแผนงานที่กำหนด ธปท. จึงขอนำส่งแผนการ Go-live BAHTNET API Phase 1 (เอกสารแนบ 1) เพื่อให้สมาชิกผู้ใช้บริการบาทเนตประสานส่วนงานภายในที่เกี่ยวข้อง ประกอบกับคู่มือธนาคารแห่งประเทศไทย พร้อมแนวปฏิบัติที่เกี่ยวข้องให้สมาชิกอ้างอิงประกอบการดำเนินการ โดยเอกสารดังกล่าวได้ผ่านการหารือและรับฟังความคิดเห็นจากผู้ใช้บริการบาทเนตแล้ว ซึ่งสรุปสาระสำคัญได้ ดังนี้

1. คู่มือ ธปท. เรื่อง การให้บริการบาทเนตผ่านช่องทาง BAHTNET API (เอกสารแนบ 2) เพื่อกำหนดขั้นตอนการดำเนินการ อาทิ การขอใช้บริการ การดำเนินการในระหว่างวันที่ใช้งาน และการดำเนินการกรณีช่องทาง API ขัดข้อง เพื่อใช้เป็นแนวทางปฏิบัติที่เป็นมาตรฐานเดียวกัน พร้อมกับนำส่งเอกสารแนบท้ายเพื่อให้ผู้มีอำนาจลงนามของสมาชิกแสดงความตกลงการใช้บริการ BAHTNET API และมอบอำนาจให้ผู้ที่เกี่ยวข้องกับการดำเนินการตามคู่มือดังกล่าว ก่อนการเริ่มใช้บริการ

2. แนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API (เอกสารแนบ 3) เพื่อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของสมาชิกในการใช้งาน และเชื่อมต่อกับ BAHTNET API ของ ธปท.

จึงเรียนมาเพื่อทราบและถือปฏิบัติ พร้อมกันนี้ ธปท. ขอขอบคุณผู้ใช้บริการระบบบาทเนตทุกสถาบันที่ให้ความร่วมอย่างดียิ่งเสมอมา

ขอแสดงความนับถือ

(นายอนรรฆ สมคะเน)
ผู้อำนวยการอาวุโส ฝ่ายกลยุทธ์และพัฒนาโครงสร้างพื้นฐานและบริการ
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย 1. แผนการ Go-live BAHTNET API Phase 1
2. คู่มือ ธปท. เรื่อง การให้บริการบาทเนตผ่านช่องทาง BAHTNET API
3. แนวปฏิบัติ เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API

ฝ่ายกลยุทธ์และพัฒนาโครงสร้างพื้นฐานและบริการ
โทรศัพท์ 0 2356 7699
ไปรษณีย์อิเล็กทรอนิกส์ saraban@bot.or.th และ BAHTNET-NextGen-BOT@bot.or.th

แผนการ Go-live BAHTNET API Phase 1

วันที่	ลำดับ	รายละเอียด	ผู้ดำเนินการ	ช่องทางการสื่อสาร
1. กิจกรรมช่วงเตรียมการ Go-live Phase 1 (1 – 11 ก.ย. 69)				
1 – 11 ก.ย. 69	1	สมาชิกเตรียมความพร้อมด้านระบบงาน และลงนามเอกสารที่เกี่ยวข้องสำหรับการ Go-Live BAHTNET API Phase 1 ดังนี้ 1. เตรียมความพร้อมด้านระบบงาน (Production Environment) เช่น จัดเตรียมเครื่อง API Client, Certificate และ Allow Firewall 2. ลงนามในเอกสารที่เกี่ยวข้อง (ฉบับจริง) ดังนี้ 2.1 ผู้มีอำนาจลงนามลงนาม “หนังสือแสดงความตกลงใช้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน” 2.2 ผู้มีอำนาจลงนามลงนาม “หนังสือแต่งตั้งผู้มีอำนาจลงนามแต่งตั้งผู้รับรอง (Certifier)” 2.3 ผู้มีอำนาจลงนามลงนาม “หนังสือแสดงความตกลงใช้บริการ BAHTNET API” 2.4 ผู้มีอำนาจลงนามลงนาม “หนังสือมอบอำนาจตามคู่มือธนาคารแห่งประเทศไทย เรื่อง การให้บริการบาทเนตผ่านช่องทาง BAHTNET API” 2.5 ผู้รับมอบอำนาจตามหนังสือมอบอำนาจบาทเนต B2.1 ข้อ 4 ลงนาม “หนังสือขอเปลี่ยนแปลงข้อมูลผู้ใช้บริการบาทเนต” ทั้งนี้ เมื่อดำเนินการลงนามแล้วเสร็จ ให้นำส่งเอกสารฉบับจริงมายัง ธปท. ตามเงื่อนไขที่กำหนด	สมาชิก	-
1 – 11 ก.ย. 69	2	เข้าร่วมการทดสอบ Go-live Rehearsal Phase 1	ธปท. สมาชิก	
11 ก.ย. 69	3	รวบรวมผลการทดสอบ Go-live Rehearsal Phase 1 ของสมาชิก	ธปท.	

2. กิจกรรมช่วง Deployment ภายใน ธปท. (11 ก.ย. 69)				
11 ก.ย. 69	4	Deploy ระบบงาน BAHTNET API Phase 1 (Production)	ธปท.	
	5	ทดสอบ DVT และ FVT โดยไม่ส่งรายการจริง	ธปท.	
	6	รวบรวมผลการตรวจสอบ DVT&FVT ของ ธปท.	ธปท.	
	7	**แจ้งความพร้อมให้บริการระบบ BAHTNET API Phase 1 ในวันที่ 14 กันยายน 2569** ให้สมาชิกทราบ	ธปท.	E-mail
3. กิจกรรมช่วง Deployment ของสมาชิก (14 ก.ย. 69 – 9 ต.ค. 69)				
14 ก.ย. 69	8	ตรวจสอบความพร้อมของระบบงาน	ธปท.	
	9	**ระบบ BAHTNET API Phase 1 เริ่มเปิดให้บริการ (7.30 – 18.30 น.)**	ธปท.	
14 ก.ย. 69 – 9 ต.ค. 69	10	1. Deploy ระบบงาน Production 2. Onboarding ผ่านระบบงาน Production ของ ธปท. ดังนี้ - Certifier/Officer จัดทำคำขอสมัครใช้บริการบนระบบ BOT API Portal และ BAHTNET API Authentication - ผู้รับมอบอำนาจ (ตามลำดับที่ 1 ข้อ 2.2) ลงนามในหนังสือแต่งตั้ง Certifier/Officer ตามเอกสารที่ได้รับจากระบบ BAHTNET API Authentication - Certifier นำส่ง certificate และ/หรือ ข้อมูลเครื่องปฏิบัติงานผ่านระบบ BAHTNET API Authentication - Certifier/Officer สมัครใช้บริการผ่านระบบ BOT API Portal 3. ทดสอบการเชื่อมต่อของระบบงานตาม Test Scenario ที่กำหนด ดังนี้ - ส่งและรับข้อความเพื่อทดสอบการเชื่อมต่อผ่าน Production Environment (Mandatory)	สมาชิก	

		- ส่งข้อความอื่น ๆ เพื่อตรวจสอบ Format และ Authorization Token ของ HTTP Header (Optional)		
14 ก.ย. 69 – 9 ต.ค. 69	11	แจ้งผลการทดสอบ Go-live Phase 1	สมาชิก	BOT Survey
14 ก.ย. 69 – 9 ต.ค. 69	12	รวบรวมผลการทดสอบ Go-live Phase 1 ของสมาชิก	ธปท.	

คู่มือธนาคารแห่งประเทศไทย
เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API

---

1. ความเป็นมา

ด้วยธนาคารแห่งประเทศไทย (ธปท.) ได้พัฒนาระบบการรับและส่งข้อความในการทำธุรกรรมผ่านระบบบาทเนต โดยใช้เครือข่ายภายในประเทศด้วยเทคโนโลยี API (BAHTNET Application Programming Interface : BAHTNET API) เพื่อเป็นโครงสร้างพื้นฐานที่สำคัญในการทำธุรกรรมผ่านระบบบาทเนตให้มีประสิทธิภาพมากขึ้น รองรับการทำงานในลักษณะ Straight Through Processing ลดความเสี่ยงในกระบวนการทำงาน และสามารถต่อยอดบริการหรือนวัตกรรมการชำระเงินในอนาคต

BAHTNET API เป็นช่องทางการรับและส่งข้อความระหว่าง ธปท. กับผู้ใช้บริการบาทเนต เป็นการส่งคำสั่งโอนเงินผ่านการให้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน (Electronic Financial Services via Certified Servers) สำหรับการทำธุรกรรมผ่านระบบบาทเนต มีข้อกำหนดและขั้นตอนการดำเนินการเพิ่มเติมจากปัจจุบัน อาทิ การขอใช้บริการ การดำเนินการในระหว่างวันที่ใช้งาน และการดำเนินการกรณี BAHTNET API ขัดข้อง ธปท. จึงออกคู่มือฉบับนี้เพื่อให้ผู้ใช้บริการบาทเนตใช้เป็นแนวทางปฏิบัติงานให้เป็นมาตรฐานเดียวกัน

2. หลักเกณฑ์ที่อ้างอิง

เพื่อให้เป็นไปตามข้อ 34 วรรคสอง ประกอบกับข้อ 94 (3) และ (4) แห่งระเบียบธนาคารแห่งประเทศไทยว่าด้วยบริการบาทเนต พ.ศ. 2549

3. ขอบเขตการบังคับใช้

ผู้ใช้บริการบาทเนต ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยบริการบาทเนต

4. เนื้อหา

4.1 นิยาม

“ธปท.” หมายถึง ธนาคารแห่งประเทศไทย

“บาทเนต” หมายถึง ระบบบาทเนตตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต

“ผู้ใช้บริการบาทเนต” หมายถึง ผู้ใช้บริการบาทเนตตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต

“BAHTNET API” (BAHTNET Application Programming Interface) หมายถึง ระบบการรับและส่งข้อความระหว่าง ธปท. กับผู้ใช้บริการบาทเนตผ่านเทคโนโลยี API

“ผู้ใช้บริการ BAHTNET API” หมายถึง ผู้ใช้บริการบาทเนตที่ทำธุรกรรมผ่าน BAHTNET API

“BOT API Portal” หมายถึง ระบบสำหรับการลงทะเบียนเพื่อขอใช้ BAHTNET API

"BNAPI-Authen" (BAHTNET API Authentication) หมายถึง ระบบสำหรับผู้ใช้บริการบาทเนตใช้ในการลงทะเบียน การยืนยันตัวตน และการบริหารจัดการข้อมูลต่าง ๆ เพื่อการใช้งาน BAHTNET API

"ผู้รับผิดชอบสูงสุดจากหน่วยงานเทคโนโลยีสารสนเทศ" หมายถึง บุคคลที่ดูแลทั้งหน่วยงานเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งได้รับมอบหมายจากผู้มีอำนาจลงนามของผู้ใช้บริการ BAHTNET API ให้เป็นผู้ส่งคำขอต่อ ธปท. ในการขอกลับมาใช้ BAHTNET API ตามปกติ ภายหลังถูกระงับใช้บริการเป็นการชั่วคราว ตามเงื่อนไขที่กำหนดในพิธีปฏิบัติกรณีฉุกเฉินของระบบบาทเนต

"ผู้รับรอง (Certifier)" หมายถึง บุคคลที่ได้รับมอบหมายจากผู้มีอำนาจลงนาม ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการให้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน (Electronic Financial Services via Certified Servers)

"ผู้ปฏิบัติงาน (Officer)" หมายถึง บุคคลที่ได้รับมอบหมายจากผู้รับรอง (Certifier) ตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการให้บริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน (Electronic Financial Services via Certified Servers)

"ใบรับรองอิเล็กทรอนิกส์ (Certificate)" หมายถึง ข้อมูลอิเล็กทรอนิกส์ที่ออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ ที่ได้รับการรับรองและกำกับดูแลโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือหน่วยงานที่เกี่ยวข้อง เพื่อใช้ในการยืนยันตัวบุคคลหรือองค์กรว่าเป็นผู้กระทำธุรกรรมอิเล็กทรอนิกส์นั้นจริง

"คอมพิวเตอร์ลูกข่าย BAHTNET API" หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต ที่ใช้เชื่อมโยงกับ BAHTNET API ของ ธปท. แบบ Host to Host ผ่านเครือข่ายเฉพาะที่ ธปท. กำหนด

4.2 หลักเกณฑ์ในการใช้บริการ BAHTNET API

4.2.1 การดำเนินการของ ธปท.

ธปท. จะจัดทำรายละเอียดบริการ มาตรฐานข้อความ ข้อกำหนดด้านการปฏิบัติงานและด้านเทคนิค รวมทั้งคู่มือที่เกี่ยวข้องให้แก่ผู้ใช้บริการบาทเนต

4.2.2 การดำเนินการของผู้ใช้บริการ BAHTNET API

ก่อนเริ่มใช้บริการ BAHTNET API ต้องดำเนินการ ดังนี้

(1) ทดสอบการใช้งาน BAHTNET API ในระบบทดสอบของ ธปท. ให้มีความพร้อมตามเงื่อนไขและวิธีการที่ ธปท. กำหนด

(2) ยื่นหนังสือแสดงความตกลงการใช้บริการ BAHTNET API (เอกสารแนบ 1) และหนังสือมอบอำนาจตามคู่มือธนาคารแห่งประเทศไทย เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API (เอกสารแนบ 2) ต่อ ธปท.

(3) จัดเตรียมใบรับรองอิเล็กทรอนิกส์ (Certificate) และรับรองเครื่องปฏิบัติงานที่เกี่ยวข้องกับการใช้บริการ BAHTNET API ตามเงื่อนไขที่ ธปท. กำหนด โดยถือปฏิบัติตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน (Electronic Financial Services via Certified Servers)

ผู้ใช้บริการต้องดูแลเครื่องปฏิบัติงานและใบรับรองอิเล็กทรอนิกส์ (Certificate) ให้พร้อมใช้งานตลอดเวลาที่ใช้บริการ BAHTNET API

(4) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยทางสารสนเทศสำหรับการใช้บริการ BAHTNET API เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นตามแนวปฏิบัติเรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต เพื่อการใช้งาน BAHTNET API

(5) ลงทะเบียนแต่งตั้งผู้รับรอง (Certifier) หรือแต่งตั้งผู้ปฏิบัติงาน (Officer) ผ่านระบบ BNAPI-Authen และให้ผู้รับรอง (Certifier) หรือผู้ปฏิบัติงาน (Officer) ลงทะเบียนผ่านระบบ BOT API Portal หรือระบบอื่นใดตามเงื่อนไข และวิธีการที่ ธปท. กำหนดเพื่อขอใช้บริการ BAHTNET API

(6) เมื่อดำเนินการตาม (5) แล้ว ให้ผู้รับรอง (Certifier) รับรองเครื่องปฏิบัติงาน และ/หรือ นำส่งใบรับรองอิเล็กทรอนิกส์ (Certificate) ที่เกี่ยวข้องกับ BAHTNET API ผ่านระบบ BNAPI-Authen หรือระบบอื่นใดตามเงื่อนไข และวิธีการที่ ธปท. กำหนด

ทั้งนี้ การปฏิบัติตามขั้นตอนดังกล่าวต้องเป็นไปตามที่ ธปท. กำหนดตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ผ่านเครื่องปฏิบัติงาน (Electronic Financial Services via Certified Servers) ด้วย

4.2.3 การให้บริการ BAHTNET API

(1) ประเภทบริการ และกรอบเวลาการให้บริการ BAHTNET API เป็นไปตามที่ ธปท. กำหนดในเอกสาร BAHTNET API Message Specification and Operational Guide

(2) การส่งข้อความหรือคำสั่งโอนเงินของผู้ใช้บริการบาทเนตผ่าน BAHTNET API จะถือว่าส่งถึงระบบบาทเนตของ ธปท. เรียบร้อยเมื่อได้รับการตอบกลับผลสำเร็จ (Success Response) จาก BAHTNET API ของ ธปท. เท่านั้น โดยหากได้รับการตอบกลับการปฏิเสธ (Error Response) จาก BAHTNET API ของ ธปท. จะถือว่าข้อความหรือคำสั่งโอนเงินดังกล่าวยังส่งไม่ถึงระบบบาทเนตของ ธปท.

(3) การส่งข้อความของ ธปท. ผ่าน BAHTNET API ไปยังผู้ใช้บริการบาทเนต จะถือว่าผู้ใช้บริการบาทเนตได้รับข้อความดังกล่าวเมื่อ BAHTNET API ของ ธปท. ได้รับการตอบกลับผลสำเร็จ (Success Response) จาก BAHTNET API ของผู้ใช้บริการบาทเนตเท่านั้น โดยหาก BAHTNET API ของ ธปท. ได้รับการตอบกลับการปฏิเสธ (Error Response) หรือ ไม่ได้รับการตอบกลับ จาก BAHTNET API ของผู้ใช้บริการบาทเนต จะถือว่าผู้ใช้บริการบาทเนตไม่ได้รับข้อความของ ธปท. และ ธปท. จะดำเนินการตามกระบวนการจัดการข้อยกเว้น (Exception Handling) ที่กำหนดในเอกสาร BAHTNET API Message Specification and Operational Guide

ทั้งนี้ กรณีที่ BAHTNET API ของ ธปท. หรือของผู้ใช้บริการบาทเนตขัดข้องทำให้ผู้ใช้บริการบาทเนตไม่สามารถรับข้อความจาก ธปท. ผ่าน BAHTNET API ภายในเวลาทำการของระบบบาทเนตได้ ให้ผู้ใช้บริการบาทเนตเรียกดูข้อมูลดังกล่าวผ่านช่องทาง BAHTNET Web Service หรือช่องทางอื่นใดที่ ธปท. กำหนด

4.2.4 การดำเนินการระหว่างวันที่ใช้บริการ BAHTNET API

ผู้ใช้บริการบาทเนตต้องตรวจสอบสถานะการเชื่อมต่อ และการทำงานของใบรับรองอิเล็กทรอนิกส์ (Certificate) กับ BAHTNET API ของ ธปท. ตามที่ ธปท. กำหนดภายใต้เอกสาร BAHTNET API Message Specification and Operational Guide

4.2.5 ค่าธรรมเนียมในการใช้บริการและค่าปรับ

ผู้ใช้บริการบาทเนตต้องชำระค่าธรรมเนียมในการใช้บริการและค่าปรับตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่ ธปท. กำหนดตามประกาศธนาคารแห่งประเทศไทยว่าด้วยเรื่องค่าธรรมเนียมและค่าปรับบริการบาทเนต

4.2.6 การระงับหรือเพิกถอนการใช้บริการ BAHTNET API

การระงับการใช้บริการ เกิดขึ้นด้วยสาเหตุ ดังนี้

(1) กรณีผู้ใช้บริการบาทเนตต้องการระงับใช้บริการ BAHTNET API ไม่ว่าเป็นการชั่วคราว (ไม่รวมถึงกรณีระบบงานขัดข้อง) หรือขอออกจากการใช้บริการ BAHTNET API ให้ผู้ใช้บริการบาทเนตแจ้งความประสงค์ต่อ ธปท. ล่วงหน้าอย่างน้อย 30 วัน ตามแบบฟอร์มที่กำหนดตามระเบียบธนาคารแห่งประเทศไทยว่าด้วยการบริการบาทเนต โดยผู้ใช้บริการบาทเนตต้องรับผิดชอบในข้อความหรือคำสั่งโอนเงินของตนเองที่ ธปท. ได้รับก่อนที่ ธปท. จะระงับการใช้บริการ

ธปท. จะพิจารณาให้ผู้ใช้บริการบาทเนตระงับใช้บริการ BAHTNET API เป็นการชั่วคราว หรือให้ออกจากการใช้บริการ BAHTNET API ตามเหตุผลและความจำเป็นของผู้ใช้บริการบาทเนต

(2) ธปท. สั่งระงับหรือเพิกถอนการใช้บริการ

(2.1) ธปท. อาจพิจารณาให้ผู้ใช้บริการบาทเนตรายใดรายหนึ่งระงับการใช้บริการ BAHTNET API เป็นการชั่วคราวเนื่องจากสาเหตุต่าง ๆ ดังต่อไปนี้

(2.1.1) ไม่ปฏิบัติตามกฎเกณฑ์ของ ธปท. ตามคู่มือฉบับนี้

(2.1.2) มีพฤติการณ์ที่อาจก่อให้เกิดผลกระทบต่อการใช้บริการบาทเนตในภาพรวม เช่น

- ส่งคำสั่งโอนเงินผ่าน BAHTNET API เกินจำนวนที่ ธปท. กำหนดอย่างมีนัยสำคัญ
- ส่งคำสั่งโอนเงินผ่าน BAHTNET API โดยระบุข้อมูลไม่ถูกต้องเกินจำนวนที่ ธปท. กำหนด
- ส่งคำสั่งโอนเงินผ่าน BAHTNET API โดยระบุข้อมูลที่อาจเป็นอันตราย (Malicious Request) ต่อระบบงานของ ธปท.

ทั้งนี้ การแจ้งขอกลับมาใช้บริการ BAHTNET API ตามปกติโดยผู้รับผิดชอบสูงสุดจากหน่วยงานเทคโนโลยีสารสนเทศ หรือผู้รับรอง (Certifier) ให้เป็นไปตามที่ ธปท. กำหนดในพิธีปฏิบัติกรณีฉุกเฉินของระบบบาทเนต

(2.2) ธปท. อาจพิจารณาเพิกถอนการให้บริการ BAHTNET API แก่ผู้ใช้บริการบาทเนตรายใดรายหนึ่งเนื่องจากสาเหตุต่าง ๆ ดังต่อไปนี้

(2.2.1) ธปท. สั่งระงับการใช้บริการ BAHTNET API เป็นการชั่วคราวด้วยเหตุผลตามข้อ (2.1) และผู้ใช้บริการบาทเนตไม่ได้ทำการแก้ไขข้อบกพร่อง หรือไม่สามารถเสนอแผนงานที่ชัดเจนสำหรับการแก้ไขข้อบกพร่องดังกล่าวภายในระยะเวลา 1 เดือน นับจากวันที่ ธปท. สั่งระงับการใช้บริการ

(2.2.2) ผู้ใช้บริการบาทเนตมีพฤติกรรมที่อาจก่อให้เกิดความเสียหายต่อการใช้บริการบาทเนตหรือเสถียรภาพของระบบการเงินโดยรวม

4.3 การดำเนินการกรณี BAHTNET API ขัดข้อง

ผู้ใช้บริการบาทเนตและ ธปท. ต้องจัดให้มีแผนฉุกเฉินตามมาตรฐานรองรับกรณี BAHTNET API ขัดข้อง เพื่อให้ธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง โดยผู้ใช้บริการบาทเนตต้องดำเนินการตามรายละเอียดและเงื่อนไขต่าง ๆ กรณีมีเหตุขัดข้องตามพิธีปฏิบัติกรณีฉุกเฉินของระบบบาทเนต

5. วันเริ่มต้นบังคับใช้

ตั้งแต่วันที่ 2 กันยายน พ.ศ. 2569

(นายอนรรฆ สมคะเน)
ผู้อำนวยการอาวุโส ฝ่ายกลยุทธ์และพัฒนาโครงสร้างพื้นฐานและบริการ
ผู้ว่าการแทน

ฝ่ายกลยุทธ์และพัฒนาโครงสร้างพื้นฐานและบริการ
โทรศัพท์ 02 356 7699

เอกสารแนบ 1

หนังสือแสดงความตกลงใช้บริการ BAHTNET API

ทำที่.....

วันที่.....

ข้าพเจ้า..... (ชื่อ ภาษาอังกฤษ .....)
ได้รับทราบและเข้าใจข้อความตามคู่มือธนาคารแห่งประเทศไทย เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API โดยละเอียดตลอดแล้ว มีความประสงค์จะใช้บริการ BAHTNET API และผูกพันตนตามเอกสารดังกล่าวตามรายละเอียดดังต่อไปนี้

1. ข้าพเจ้าตกลงผูกพันตนกับยินยอมปฏิบัติตามหลักเกณฑ์และข้อกำหนดการใช้บริการบาทเนตผ่าน BAHTNET API ของ ธปท. ที่ใช้บังคับอยู่ขณะนี้และที่จะแก้ไขเพิ่มเติมหรือมีขึ้นในภายหน้าทุกประการ

2. ข้าพเจ้ายินยอมให้ ธปท. ระงับการใช้บริการ BAHTNET API เป็นการชั่วคราวหรือเพิกถอนการให้บริการ BAHTNET API หากพิจารณาเห็นว่าข้าพเจ้ามีพฤติการณ์ที่อาจก่อให้เกิดผลกระทบต่อการใช้บริการบาทเนตในภาพรวม

3. ข้าพเจ้าได้ส่งหนังสือมอบอำนาจตามคู่มือธนาคารแห่งประเทศไทย เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API มาพร้อมนี้

ข้าพเจ้าจะไม่เพิกถอนความตกลงตามหนังสือนี้ เว้นแต่จะได้รับความเห็นชอบจาก ธปท. เป็นหนังสือ

ลงลายมือชื่อ .....(ผู้มีอำนาจลงนาม).....

(.....)

ลงลายมือชื่อ .....(ผู้มีอำนาจลงนาม).....

(.....)

เพื่อ .....(ชื่อสถาบัน).....

<u>หมายเหตุ</u> ลงนามโดยผู้มีอำนาจลงนามตามหนังสือรับรองกระทรวงพาณิชย์ ที่มีอายุไม่เกิน 6 เดือน นับถึงวันลงนาม

เอกสารแนบ 2

หนังสือมอบอำนาจตามคู่มือธนาคารแห่งประเทศไทย
เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API

ทำที่.....
วันที่.....

ตามหนังสือแสดงความตกลงใช้บริการ BAHTNET API ของข้าพเจ้า ..... ลงวันที่ .....ซึ่งได้ตกลงผูกพันตนกับยินยอมปฏิบัติตามคู่มือธนาคารแห่งประเทศไทย เรื่อง การให้บริการบาทเนตผ่าน BAHTNET API นั้น

ข้าพเจ้าขอมอบอำนาจให้บุคคลตามรายชื่อในหนังสือนี้เป็นผู้ดำเนินการแทนข้าพเจ้า ในการดำเนินการดังต่อไปนี้

1. ขอใช้งาน BAHTNET API ภายหลังถูกระงับใช้บริการเป็นการชั่วคราว[1]
2. ติดต่อกับ ธปท. ในกิจการอื่นใดที่เกี่ยวกับบริการ BAHTNET API

ชื่อ-นามสกุล	เงื่อนไข	โทรศัพท์	Email
.....	.....	.....	.....
.....	.....	.....	.....

การใด ๆ ที่ผู้รับมอบอำนาจได้กระทำไปให้มีผลผูกพันข้าพเจ้าทุกประการ และข้าพเจ้าจะไม่เพิกถอนการมอบอำนาจตามหนังสือนี้ เว้นแต่มีการเพิ่มเติมหรือเปลี่ยนแปลงบุคคลผู้รับมอบอำนาจ ข้าพเจ้าจะแจ้งให้ ธปท. ทราบล่วงหน้าเป็นหนังสือ

ทั้งนี้ การมอบอำนาจดังกล่าวให้มีผลตั้งแต่วันที่.....เป็นต้นไป

ลงลายมือชื่อ .....(ผู้มีอำนาจลงนาม).....

(.....)

ลงลายมือชื่อ .....(ผู้มีอำนาจลงนาม).....

(.....)
เพื่อ .....(ชื่อสถาบัน).....

<u>หมายเหตุ</u> ลงนามโดยผู้มีอำนาจลงนามตามหนังสือรับรองกระทรวงพาณิชย์ และติดอากรแสตมป์ **(ท่านละ 30 บาท)**

---

[1] กรณีดังกล่าวจะเกิดขึ้นภายหลังจากที่สมาชิกถูกระงับใช้บริการ BAHTNET API เป็นการชั่วคราว เนื่องจากมีพฤติการณ์ที่อาจก่อให้เกิดผลกระทบต่อการใช้บริการบาทเนตในภาพรวม ดังนั้น บุคคลที่ได้รับมอบอำนาจให้ดำเนินการควรเป็น ผู้รับผิดชอบสูงสุดจากหน่วยงานเทคโนโลยีสารสนเทศ หรือ บุคคลที่ดูแลทั้งหน่วยงานเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

แนวปฏิบัติ

เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API

ธนาคารแห่งประเทศไทย

จัดทำโดย
ฝ่ายเทคโนโลยีสารสนเทศ
สายระบบข้อสนเทศ
ธนาคารแห่งประเทศไทย

สารบัญ

หัวข้อ **หน้า**

แนวปฏิบัติธนาคารแห่งประเทศไทย

เรื่อง การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ลูกข่าย BAHTNET API

---

1. เหตุผลในการออกแนวปฏิบัติ

ธนาคารแห่งประเทศไทย (ธปท.) ได้ดำเนินการแผนงานระบบ BAHTNET Application Programming Interface (BAHTNET API) ภายใต้โครงการ BAHTNET NextGen เพื่อปรับระบบบาทเนตให้รองรับกับความก้าวหน้าทางเทคโนโลยีที่เปลี่ยนแปลงไป โดยพัฒนา Domestic Network ที่ใช้เทคโนโลยี Application Programming Interface ซึ่งสามารถสนับสนุนให้เกิดนวัตกรรมและการต่อยอดบริการด้านการชำระเงิน รองรับการจัดการความเสี่ยง Geopolitical Risk และเป็นรากฐานของการพัฒนา New Core Infrastructure ของระบบบาทเนต (BAHTNET Modernization) ในอนาคต

ในการนี้ ธปท. จึงได้ออกแนวปฏิบัติฉบับนี้ เพื่อกำหนดแนวทางการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต เพื่อการใช้งาน BAHTNET API ให้มีแนวปฏิบัติที่ครอบคลุมและเป็นมาตรฐานเดียวกัน รวมถึงสอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีในปัจจุบัน และเสริมสร้างมาตรฐานการรักษาความมั่นคงปลอดภัยในเรื่องการควบคุมระบบคอมพิวเตอร์ เพื่อใช้เป็นกรอบแนวทางให้ผู้ใช้บริการบาทเนตนำไปปรับใช้ให้เหมาะสม และบริหารความเสี่ยงที่เกี่ยวข้องกับการทำธุรกรรมได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

ทั้งนี้ ผู้ใช้บริการบาทเนตสามารถกำหนดมาตรการรักษาความมั่นคงปลอดภัย ที่แตกต่างจากแนวปฏิบัติฉบับนี้ได้ หากมาตรการดังกล่าวมีความสอดคล้องและสามารถป้องกันความเสี่ยงของระบบคอมพิวเตอร์ได้อย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่ยอมรับได้ นอกจากนี้ ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กรตามข้อกำหนดในกฎหมาย ระเบียบ และประกาศที่เกี่ยวข้อง (ภาคผนวก 1) และให้มีการรายงานเหตุการณ์ความเสี่ยงตามที่กำหนด (ภาคผนวก 2) เพื่อให้มั่นใจว่ากระบวนการทำงานและ ธุรกรรมมีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายในปัจจุบัน และเป็นไปตาม มาตรฐานสากล รวมทั้งที่มีการปรับปรุงเพิ่มเติมหรือที่มีข้อกำหนดเพิ่มขึ้นในอนาคต

2. ขอบเขตการบังคับใช้

แนวปฏิบัตินี้เป็นกรอบแนวทางให้ผู้ใช้บริการบาทเนตใช้กำหนดมาตรการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต เครือข่าย อุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. และอุปกรณ์ Hardware Security Module (HSM) ของผู้ใช้บริการบาทเนต รวมถึงการควบคุมด้านการปฏิบัติงานและการจัดการด้านบุคลากรและการสื่อสารที่เกี่ยวข้อง

ทั้งนี้ ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการตรวจรับรองระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 อย่างต่อเนื่อง โดยครอบคลุมระบบและอุปกรณ์ดังกล่าวข้างต้น

3. เนื้อหา

3.1 ความหมาย ในแนวปฏิบัติฉบับนี้

“แนวปฏิบัติ” หมายถึง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API ของผู้ใช้บริการบาทเนต

“คอมพิวเตอร์ลูกข่าย BAHTNET API” หมายถึง ระบบคอมพิวเตอร์ของผู้ใช้บริการบาทเนต ที่ใช้เชื่อมโยงกับ BAHTNET API ของ ธปท. แบบ Host to Host ผ่านเครือข่ายเฉพาะที่ ธปท. กำหนด

“ระบบคอมพิวเตอร์” หมายถึง งานด้านเทคโนโลยีสารสนเทศที่ครอบคลุมถึง เครื่องคอมพิวเตอร์และอุปกรณ์รอบข้าง (Hardware) ระบบงาน (Application) ข้อมูล (Information) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (Infrastructure) เครือข่าย (Network) บุคลากร (People) และกระบวนการจัดการด้านเทคโนโลยีสารสนเทศ (Process)

“ศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต” หมายถึง ศูนย์คอมพิวเตอร์ที่ใช้ในการจัดเก็บคอมพิวเตอร์ลูกข่าย BAHTNET API ของผู้ใช้บริการบาทเนต โดยมีสถานที่ตั้งภายในองค์กร (On-Premises) หรือสถานที่ของผู้ให้บริการภายนอก (Off-Premises)

“ความมั่นคงปลอดภัย” หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ละเมิดต่อความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ หรือการกระทำที่มีเจตนาทำให้มีความเสี่ยง หรือก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัยของคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) รวมถึงการฉ้อโกง อันนำไปสู่ความเสียหายทางการเงิน ความเสียหายต่อชื่อเสียง และการขาดความเชื่อมั่นของผู้ใช้บริการบาทเนตต่อการให้บริการทางการเงินโดยรวม

3.2 รายละเอียดของแนวปฏิบัติ

3.2.1 การควบคุมคอมพิวเตอร์ลูกข่าย เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต รวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

(2) กำหนดวิธีการและสิทธิการเข้าถึงคอมพิวเตอร์ลูกข่าย BAHTNET API โดยจัดให้มีการแบ่งอำนาจหน้าที่ของพนักงานอย่างเหมาะสมเพื่อป้องกันมิให้พนักงานผู้ใดได้รับสิทธิอย่างเบ็ดเสร็จ และมีกระบวนการจัดการ User ที่มีสิทธิสูง (Privilege Account Management) รวมถึงทบทวนสิทธิดังกล่าวโดยสม่ำเสมอ

(3) จัดให้มีการรักษาความมั่นคงปลอดภัยของเครือข่ายที่เชื่อมโยงระหว่างคอมพิวเตอร์ลูกข่าย BAHTNET API กับ BAHTNET API ของ ธปท. เช่น การติดตั้ง Firewall เป็นต้น

(4) ควบคุมการเข้าถึงคอมพิวเตอร์ลูกข่าย BAHTNET API จากระบบงานอื่นที่ไม่จำเป็นต้องเชื่อมโยง เช่น แยกเครือข่ายคอมพิวเตอร์ลูกข่าย BAHTNET API ออกจากเครือข่ายสำหรับระบบงานภายในองค์กร เป็นต้น

(5) ไม่ใช้งานคอมพิวเตอร์ลูกข่าย BAHTNET API ร่วมกับระบบงานอื่น ยกเว้นอาจใช้ร่วมกับบริการด้านการเงินด้วยวิธีอิเล็กทรอนิกส์ของ ธปท.

หากมีระบบงานอื่นในระดับ Logical เช่น Virtual Machine ที่ต้องการใช้งานบนเครื่อง Physical Server เดียวกัน ระบบงานดังกล่าวจะต้องมีการรักษาความปลอดภัยเทียบเท่ากับคอมพิวเตอร์ลูกข่าย BAHTNET API

กรณีคอมพิวเตอร์ลูกข่าย BAHTNET API ติดตั้งที่ศูนย์คอมพิวเตอร์ที่ใช้งานร่วมกับผู้ใช้บริการรายอื่น ต้องมีการแยกการใช้งานออกจากผู้ใช้บริการรายอื่นอย่างชัดเจน ทั้งในระดับเครือข่ายและระดับ Logical เป็นอย่างน้อย เช่น การแยก VLAN และการแยก Virtual Machine

(6) อนุญาตให้เชื่อมต่อบริการหรือระบบงานอื่นที่อยู่ภายในศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนตที่จำเป็นสำหรับการปฏิบัติงาน และการรักษาความมั่นคงปลอดภัยเท่านั้น เช่น ระบบ Infrastructure พื้นฐาน เป็นต้น

(7) อนุญาตให้เชื่อมต่อบริการหรือระบบงานที่อยู่ภายนอกศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต เฉพาะ Certificate Authority และ Endpoint Protection

(8) มีกลไกป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Endpoint Protection) โดย Update Signature จากผู้ผลิตอย่างสม่ำเสมอ และมีการทำ Scheduled Scan ตามระยะเวลาที่เหมาะสม

สำหรับคอมพิวเตอร์ลูกข่าย BAHTNET API ที่ไม่สามารถติดตั้งโปรแกรมป้องกันและตรวจจับการบุกรุกของโปรแกรมประสงค์ร้าย (Endpoint Protection) ควรประเมินความเสี่ยงและมีมาตรการควบคุมทดแทน

(9) จัดให้มีการประเมินช่องโหว่ (Vulnerability Assessment) และติดตั้งโปรแกรมเพื่อปิดช่องโหว่ (Windows Security Patch) ตามกรอบเวลาการติดตั้ง Patch ขององค์กร อย่างน้อยปีละ 1 ครั้ง

(10) จัดให้มีการทดสอบเจาะระบบ (Penetration Test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(11) มีการบริหารจัดการการตั้งค่าระบบ (System Configuration Management) โดยจัดให้มีการตั้งค่าการรักษาความมั่นคงปลอดภัย (Security Hardening) เป็นไปตามมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ (Minimum Security Baseline) ขององค์กร รวมทั้งดำเนินการสอบทานการตั้งค่าอย่างสม่ำเสมอตามที่ได้กำหนดไว้

(12) มีการรักษาความมั่นคงปลอดภัยของระบบงาน (Application Security) เป็นไปตามมาตรฐานและแนวปฏิบัติขององค์กรหรือที่ได้รับการยอมรับในระดับสากล เช่น OWASP เป็นต้น

(13) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) ของคอมพิวเตอร์ลูกข่าย BAHTNET API เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท.

(14) มีคอมพิวเตอร์ลูกข่าย เครือข่าย และอุปกรณ์เครือข่ายที่เชื่อมโยงกับ BAHTNET API ของ ธปท. ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (Disaster Recovery Site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติ

งานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (primary site) หยุดชะงัก โดยต้องสอดคล้องกับระยะเวลาในการกู้คืนระบบ (Recover Time Objective : RTO) 2 ชั่วโมง และระยะเวลาการให้บริการ (Availability) ในรอบ 1 ปีปฏิทิน ควรไม่น้อยกว่า 99.90%

3.2.2 การควบคุมอุปกรณ์ Hardware Security Module (HSM)

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยอุปกรณ์ Hardware Security Module (HSM) ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) ควบคุมการเข้าถึงอุปกรณ์ Hardware Security Module (HSM) โดยกำหนดวิธีการและสิทธิการเข้าถึงอุปกรณ์ Hardware Security Module (HSM) จัดให้มีการแบ่งอำนาจหน้าที่ของพนักงานอย่างเหมาะสมเพื่อป้องกันมิให้พนักงานผู้ใดได้รับสิทธิอย่างเบ็ดเสร็จ และมีกระบวนการจัดการ User ที่มีสิทธิสูง (Privilege Account Management) รวมถึงทบทวนสิทธิดังกล่าวโดยสม่ำเสมอ

(2) อนุญาตให้เชื่อมต่อบริการหรือระบบงานอื่นที่อยู่ภายในศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนตที่จำเป็นสำหรับการปฏิบัติงาน และการรักษาความมั่นคงปลอดภัยเท่านั้น เช่น ระบบ Infrastructure พื้นฐาน เป็นต้น

(3) ไม่อนุญาตให้เชื่อมต่อบริการหรือระบบงานที่อยู่ภายนอกศูนย์คอมพิวเตอร์ของผู้ใช้บริการบาทเนต

(4) การสร้างและจัดเก็บ Key ที่ใช้สำหรับลายมือชื่อดิจิทัล รวมถึงการสร้างลายมือชื่อดิจิทัล ต้องดำเนินการในอุปกรณ์ Hardware Security Module (HSM) ที่มีมาตรฐานความปลอดภัย FIPS 140-2 Level 2 ขึ้นไป โดยมีการแบ่งแยกการจัดเก็บ Key ออกจากระบบงานอื่นภายในองค์กร เช่น แยกอุปกรณ์ HSM หรือ แยก Partition บนอุปกรณ์ HSM เป็นต้น

กรณี Key สำหรับสร้างลายมือชื่อดิจิทัล มิได้เก็บไว้ที่ผู้ใช้บริการบาทเนต แต่ถูกเก็บไว้บนอุปกรณ์ Hardware Security Module (HSM) ของผู้ให้บริการหรือหน่วยงานภายนอก อาจพิจารณาปฏิบัติตามข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยบริการลงลายมือชื่อดิจิทัลที่ใช้การควบคุมจากระยะไกล (Remote Signing) ตามประกาศสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เพิ่มเติม

(5) กำหนดวิธีการควบคุมการแก้ไขเปลี่ยนแปลง (Change Management) อุปกรณ์ Hardware Security Module (HSM)

(6) มีอุปกรณ์ Hardware Security Module (HSM) ติดตั้งที่ศูนย์คอมพิวเตอร์สำรอง (Disaster Recovery Site) ที่มีความพร้อมใช้งานและสามารถปฏิบัติงานทดแทนได้เมื่อศูนย์คอมพิวเตอร์หลัก (Primary Site) หยุดชะงัก โดยต้องสอดคล้องกับระยะเวลาในการกู้คืนระบบ (Recover Time Objective : RTO) 2 ชั่วโมง และระยะเวลาการให้บริการ (Availability) ในรอบ 1 ปีปฏิทิน ควรไม่น้อยกว่า 99.90%

3.2.3 การควบคุมด้านการปฏิบัติงาน

ผู้ใช้บริการบาทเนตต้องกำหนดมาตรการด้านการรักษาความมั่นคงปลอดภัยด้านการปฏิบัติงาน เพื่อกำหนดแนวทางติดตาม และเตรียมความพร้อมสำหรับเหตุละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) ทั้งนี้ มาตรการดังกล่าวควรครอบคลุมถึง

(1) จัดให้มีผู้รับผิดชอบด้านความมั่นคงปลอดภัย ทั้งในระดับปฏิบัติงานและระดับบริหารเพื่อติดตาม บันทึก แก้ไข และรายงานเมื่อมีการละเมิดความมั่นคงปลอดภัย

(2) จัดทำแผนฉุกเฉินกรณีที่เกิดความเสียหายจากภัยคุกคามให้ครอบคลุมกรณีการบุกรุกของ Malware รวมถึงภัยคุกคามขั้นสูง โดยกำหนดขั้นตอนการแก้ไขปัญหา ทีมงานหรือผู้รับผิดชอบ รวมถึงวิธีการรายงานปัญหาให้กับผู้บริหาร และแจ้งผู้เกี่ยวข้องทราบอย่างรวดเร็วที่สุดเท่าที่จะทำได้ เพื่อแก้ไขปัญหาให้กลับคืนสู่สภาวะปกติโดยเร็ว

(3) มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ของคอมพิวเตอร์ลูกข่าย BAHTNET API อุปกรณ์ Hardware Security Module (HSM) และระบบคอมพิวเตอร์ที่เกี่ยวข้อง ด้วยวิธีการที่ปลอดภัย โดยข้อมูลบันทึกเหตุการณ์ครอบคลุมอย่างน้อย Access log และ Activity log ที่สำคัญ รวมถึงเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Security Events) เช่น การเข้าถึงระบบ การแก้ไขปรับแต่งระบบ การทำรายการธุรกรรมที่สำคัญ เป็นต้น และมีการจัดเก็บข้อมูลอย่างน้อย 90 วัน หรือตามระยะเวลาที่กฎหมายกำหนด โดยอาจจัดให้มี Security Information Event Management (SIEM) สำหรับการบันทึก Security Events

(4) จัดให้มีการติดตาม บันทึก และรายงานเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ลูกข่าย BAHTNET API และอุปกรณ์ Hardware Security Module (HSM) ให้เป็นไปตามมาตรฐานที่ดี รวมทั้งให้มีการเรียนรู้จากเหตุการณ์ที่เกิดขึ้นเพื่อเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า โดยครอบคลุมถึง

(4.1) แนวทางในการรับรู้ปัญหาที่เกิดขึ้นอย่างทันท่วงที โดยใช้ข้อมูลและเครื่องมือที่พัฒนาขึ้นตามกรอบแนวความเสี่ยง (Risk-Based Approach) และวิธีการอื่นใด เพื่อยับยั้ง ตรวจจับ ระบุ และสกัดกั้นเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย

(4.2) กำหนดขั้นตอนการแก้ไขปัญหา วิธีการรายงานปัญหาให้กับผู้บริหาร วิธีการแจ้งให้ ธปท. และผู้เกี่ยวข้องทราบ รวมถึงวิธีการติดตามการแก้ไขปัญหา รวมทั้งกำหนดทีมงานหรือผู้รับผิดชอบที่สามารถติดต่อได้ในกรณีเร่งด่วน ทั้งในและนอกเวลาทำการ เพื่อให้สามารถปฏิบัติงานได้อย่างทันท่วงทีเมื่อมีการร้องขอ

(4.3) เก็บรวบรวมหลักฐานต่าง ๆ ที่เป็นประโยชน์

(4.4) บันทึกเหตุการณ์หรือจัดทำรายงานที่เป็นลายลักษณ์อักษร ซึ่งรวมถึงติดตามและตรวจสอบความผิดปกติของบันทึกเหตุการณ์ที่ละเมิดต่อความมั่นคงปลอดภัย เพื่อใช้เป็นแนวทางในการแก้ปัญหา รวมทั้งทบทวนความเหมาะสมของแนวทางปัจจุบัน และพิจารณาปรับปรุงมาตรการที่จำเป็นเพิ่มเติม

3.2.4 การจัดการด้านบุคลากรและการสื่อสาร

ผู้ใช้บริการบาทเนตต้องจัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่เกิดขึ้นอย่างใกล้ชิด รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล และประชาสัมพันธ์วิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ ทั้งภายในและภายนอกองค์กร ได้แก่

(1) จัดให้มีการพัฒนา ฝึกอบรม และให้ความรู้อย่างต่อเนื่องแก่ผู้บริหารและพนักงานทุกระดับ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบคอมพิวเตอร์โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ (Security Awareness) เช่น จัดการอบรมเพิ่มเติมความรู้ให้แก่บุคลากรเก่าและใหม่อย่างสม่ำเสมอ และจัดให้มีการประชาสัมพันธ์เพื่อรณรงค์ให้ไม่เปิดอีเมล์ที่ต้องสงสัยหรือไม่เข้า Web Site ที่ไม่เหมาะสม เป็นต้น

(2) จัดให้มีการประชาสัมพันธ์ให้ข้อมูลและคำแนะนำที่เป็นประโยชน์แก่ลูกค้าผู้ใช้บริการบาทเนต เช่น วิธีการใช้บริการอย่างปลอดภัย เป็นต้น

(3) จัดให้มีการติดตามพัฒนาการทางเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่อาจก่อให้เกิดเหตุการณ์ละเมิดต่อความมั่นคงปลอดภัยอย่างใกล้ชิด มีการหารือร่วมกับผู้เชี่ยวชาญทางด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ รวมทั้งสื่อสาร แลกเปลี่ยนข้อมูล เพื่อกำหนดวิธีการป้องกันภัยคุกคามต่อระบบคอมพิวเตอร์ทั้งภายในและภายนอกองค์กร และประชาสัมพันธ์ให้ผู้เกี่ยวข้องทราบ

4. วันเริ่มต้นบังคับใช้

แนวปฏิบัติฉบับนี้ให้ใช้ตั้งแต่วันที่ 2 กันยายน 2569 เป็นต้นไป

ภาคผนวก 1

กฎหมายที่เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์และข้อกำหนดที่เกี่ยวข้อง[1/]

ผู้ใช้บริการบาทเนตต้องดำเนินการให้มีการรักษาความมั่นคงปลอดภัยในองค์กร ดำเนินการตามกฎหมายควบคุมการประกอบธุรกิจอื่น ๆ เพื่อให้มั่นใจว่ากระบวนการทำงานและธุรกรรม มีการรักษาความมั่นคงปลอดภัยที่ดี สอดคล้องกับข้อกำหนดตามกฎหมายที่เกี่ยวข้อง และเป็นไปตามมาตรฐานสากล มีตัวอย่างดังนี้

1. **พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และที่แก้ไขเพิ่มเติม**
2. **พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549**
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ (ฉบับที่ 2) พ.ศ. 2556
3. **พระราชบัญญัติระบบการชำระเงิน พ.ศ. 2560**
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 1/2561 เรื่อง หลักเกณฑ์การกำกับดูแลผู้ให้บริการระบบการชำระเงินที่มีความสำคัญ
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนช. 2/2561 เรื่อง หลักเกณฑ์การกำกับดูแลสมาชิกของระบบการชำระเงินที่มีความสำคัญ
4. **พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553**
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555
   - ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. 2555
5. **ระเบียบ ประกาศ แนวปฏิบัติของธนาคารแห่งประเทศไทย**
   - ระเบียบธนาคารแห่งประเทศไทย ว่าด้วยการบริการบาทเนต
   - ประกาศธนาคารแห่งประเทศไทย ที่ สรข. 4/2560 เรื่อง มาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคอมพิวเตอร์ลูกข่ายระบบบาทเนต
   - ประกาศธนาคารแห่งประเทศไทย ที่ สกช. 5/2566 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) ของสถาบันการเงินและสถาบันการเงินเฉพาะกิจ
   - ประกาศธนาคารแห่งประเทศไทย ที่ สนส. 27/2551 เรื่อง การอนุญาตให้บริษัทเงินทุนและบริษัทเครดิตฟองซิเอร์ให้บริการการเงินทางอิเล็กทรอนิกส์

---

[1] ธปท. ได้ทำการรวบรวมมาจากกฎหมาย ประกาศ รวมถึงหนังสือเวียน แนวปฏิบัติ และแนวนโยบายของธนาคารแห่งประเทศไทยที่มีผลใช้บังคับ ณ สิ้นเดือนธันวาคม พ.ศ. 2567 แต่อาจไม่ครอบคลุมทั้งหมด ทั้งนี้ หากกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่เกี่ยวข้องตามที่ปรากฏในภาคผนวกนี้ได้มีการปรับปรุงแก้ไขเพิ่มเติม ให้ถือปฏิบัติตามกฎหมาย ประกาศ หนังสือเวียน แนวปฏิบัติ และแนวนโยบายที่ได้มีการแก้ไขเพิ่มเติมนั้น

- แนวปฏิบัติในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่ ฝตท.(01) ว. 20/2566 และที่แก้ไขเพิ่มเติม
- แนวปฏิบัติการบริหารจัดการความเสี่ยงจากบุคคลภายนอก ที่ ฝตท.(01) ว. 20/2566 และที่แก้ไขเพิ่มเติม

6. **ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์**

ภาคผนวก 2

เกณฑ์การรายงานเหตุการณ์ความเสี่ยง

หากผู้ใช้บริการบาทเนตพบว่ามีคำสั่งโอนเงินที่ส่งเข้าระบบบาทเนตจากสถาบันของตน ซึ่งเข้าข่ายธุรกรรมทุจริต ผู้ใช้บริการบาทเนตมีหน้าที่ต้องรายงานเหตุการณ์ดังกล่าว ให้ ธปท. ทราบ ทั้งนี้ มีเกณฑ์เหตุการณ์ทุจริตที่ต้องรายงาน ดังนี้

1. มีโอกาสสร้างความเสียหายด้านข้อมูล ตัวเงินอย่างมีนัยสำคัญ รวมถึงผลกระทบด้านการรับรู้ และความเชื่อมั่นต่อสาธารณชน
2. อาจกระทบต่อเสถียรภาพระบบสถาบันการเงิน
3. อาจส่งผลกระทบต่อการให้บริการ ระบบ หรือ ชื่อเสียงของสถาบันการเงิน
4. มีการรายงานต่อผู้บริหารในระดับ Manager or Compliance Department

---